SIGN IN

RISK ASSESSMENT —

Record-breaking DDoS reportedly delivered by >145k hacked cameras

Once unthinkable, 1 terabit attacks may soon be the new normal.

DAN GOODIN - 9/28/2016, 8:50 PM

Last week, security news site KrebsOnSecurity went dark for more than 24 hours following what was believed to be a record 620 gigabit-per-second denial of service attack brought on by an ensemble of routers, security cameras, or other so-called Internet of Things devices. Now, there's word of a similar attack on a French Web host that peaked at a staggering 1.1 terabits per second, more than 60 percent bigger.

The attacks were first reported on September 19 by Octave Klaba, the founder and CTO of OVH. The first one reached 1.1 Tbps while a follow-on was 901 Gbps. Then, last Friday, he reported more attacks that were in the same almost incomprehensible range. He said the distributed denial-of-service (DDoS) attacks were delivered through a collection of hacked Internet-connected cameras and digital video recorders. With each one having the ability to bombard targets with 1 Mbps to 30 Mbps, he estimated the botnet had a capacity of 1.5 Tbps.

On Monday, Klaba reported that more than 6,800 new cameras had joined the botnet and said further that over the previous 48 hours the hosting service was subjected to dozens of attacks, some ranging

from 100 Gbps to 800 Gbps. On Wednesday, he said more than 15,000 new devices had participated in attacks over the past 48 hours.

FURTHER READING
Why the silencing of KrebsOnSecurity opens a troubling chapter for the 'Net

DDoS mitigation experts haven't confirmed the numbers, and Klaba didn't respond to a request for an interview. Still, his account is believable and largely squares with what's being reported by Akamai, the company that until recently fought the record-breaking attacks directed at KrebsOnSecurity. Indeed, Klaba said evidence suggests his network and KrebsOnSecurity may be targeted by the same botnet. But even if they're different botnets, the events over the past week are likely to set a new precedent for DDoS attacks.

"Now that we've seen a 600 gig botnet, we have to plan that within one to two years, those are going to become common," Martin McKeay, a member of Akamai's security intelligence team, told Ars. "They may not be every attack, but we will see a dozen of them a quarter, we'll see a couple hundred of them a year. Now that people know those are a possibility, they're going to start pushing in that direction. They're going to make it happen."

Prior to last week, the biggest DDoS attack Akamai had mitigated was one in June that peaked at 363 Gbps.

FURTHER READING
Large botnet of CCTV devices knock the snot out of jewelry website

Security experts have been warning for years that Internet-connected devices posed a potential threat. In early 2015, the threat was finally confirmed with evidence showing that DDoSes that disrupted Sony's PlayStation Network and Microsoft's Xbox Live were largely powered by home routers that had been hacked and corralled into a powerful botnet. In June, researchers at security firm Sucuri uncovered a botnet of 25,000 closed-circuit TVs bombarding a brick-and-mortar jewelry store.

It's not easy for most people to know if their routers, DVRs, and other Internet-connected devices are infected. Most come with only a minimal control panel, and it's not possible to use antivirus software to scan them for infections. Depending on the type of attack they're carrying out, devices may show no sign they're taking part in a crippling DDoS. The most important things end users can do is to change all default passwords, or better yet, to never connect the devices to the Internet in the first place. Of course, a connectionless router or modem won't be of any use, but often closed-circuit TV cameras work just fine without a connection. With no easy remedy for the growing epidemic of infected devices, people should be prepared for attacks that have the ability to disrupt ever bigger swaths of the Internet.

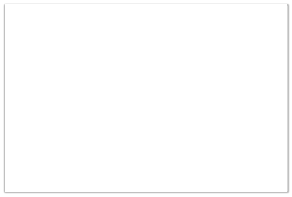
"It's getting huge," Akamai's McKeay said of the recently reported attack volumes. "You're going to see brownouts, sections where a data center, an ISP, a region, may have so much traffic that it takes down that region."

DAN GOODIN
Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

← PREVIOUS STORY NEXT STORY →

Related Stories

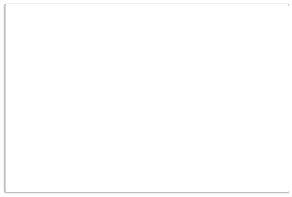
Today on Ars



Zoology review: A tail of individuality in oppressive Russia

AT&T and Time Warner reveal merger to create ISP, TV, and media giant

AT&T has $80 billion deal to purchase Time Warner Inc. (and with it, HBO)



Pediatricians revise thinking on screen time; ditch ban for kids under 2

NY governor approves fines for some rental ads—hours later, Airbnb sues

Essen 2016: Best board games from the biggest board game convention

Talking the good and bad of racing technology with Stefan Johansson

BMW Films is back with *The Escape*, premiering on Sunday

RSS FEEDS
VIEW MOBILE SITE
VISIT ARS TECHNICA UK
ABOUT US
CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS